UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,960	09/05/2003	Takashi Enami	242325US2	7967

22850 7590 04/22/2011

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
MAI, KEVIN S	

ART UNIT	PAPER NUMBER
2456	

NOTIFICATION DATE	DELIVERY MODE
04/22/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/654,960	ENAMI ET AL.	
	Examiner	Art Unit	
	KEVIN S. MAI	2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action has been issued in response to Applicant's Amendment filed April 7, 2011.

2. Claims 1-30 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed April 7, 2011 have been fully considered but they are not persuasive.

4. Applicant's arguments with respect to claim 1 have been considered but they are not persuasive. Applicants argues the references fail to disclose checking if an address of a file receiving terminal matches the stored address. However, applicant's arguments are directed solely toward Hansen and fail to address Tretter. Both references were used to disclose the argued limitation and as such it is seen that the combination of Hansen and Tretter still disclose the claimed invention. Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM

of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

5. Applicant argues that nowhere does Hansen describe that the mobile computing device transfers an address of the printing station to server. Examiner disagrees. Paragraph [0035] of Hansen discloses computer 154 is used (via printing menu 120 and user interface 17) to identify the document and upload the document via network communication link 20 to secure commercial server 160 (via commercial website 162) for future printing. Next, the user optionally identifies which commercial printer 164 of the commercial printing system 150 will print the document.

6. Applicant argues that applicant's invention provides at least the non obvious advantageous effect of improving security of a system in which files are transmitted via a server. However, because Hansen describe that the printing instructions are sent from a mobile computing device to a printing station, Hansen lacks the above-noted advantageous feature. Examiner disagrees. Figure 6 of Hansen clearly discloses a document is posted at a secure server (304) and then a printer securely gets the print job from the server (310). As such Hansen clearly discloses a system that improves security of a system in which files are transmitted via a server.

7. The remaining arguments are similar to those recited previously and as such examiner has reproduced the previous response to arguments.

8. Applicant's arguments with respect to claim 1 have been considered but they are not persuasive. Applicant argues that Hansen fails to disclose the file management server is configured to store and to correlatingly manage the address of said particular file receiving

terminal with the file. Examiner disagrees. Paragraph [0035] of Hansen discloses computer 154 is used (via printing menu 120 and user interface 17) to identify the document and upload the document via network communication link 20 to secure commercial server 160 (via commercial website 162) for future printing. Next, the user optionally identifies which commercial printer 164 of the commercial printing system 150 will print the document. Accordingly it is seen that since a user has informed the commercial server that they wish for the document to be printed by a specific printer the two are managed correlatingly. Additionally since this is done at the time of uploading the file this information would be stored until the print job was called upon.

9. Applicant further argues that Hansen fails to disclose in response to the request transmitted by said file receiving terminal, if an address of said file receiving terminal and the address of the particular file receiving terminal transferred by the mobile terminal are determined to match, and if the request transmitted by said file receiving terminal is determine to include the second password, said file management server is configured to transfer the file to said file receiving terminal. Examiner disagrees. Paragraph [0035] of Hansen discloses computer 154 is used (via printing menu 120 and user interface 17) to identify the document and upload the document via network communication link 20 to secure commercial server 160 (via commercial website 162) for future printing. Next, the user optionally identifies which commercial printer 164 of the commercial printing system 150 will print the document. Accordingly it is seen that since a user has informed the commercial server that they wish for the document to be printed by a specific printer the two are managed correlatingly. Paragraph [0040] of Hansen discloses the mobile computing device 210 delivers to printing station 208 a security key and printing instructions to activate printer 220. With the support of computer 224, printer 220 obtains access

to document from server 202 with the security key, retrieves the document, and then using the printing instructions, prints the document on printer 220. Thus the printer is seen to request the document. Then as shown above the user is able to identify which printer is to print the document at the time of upload and accordingly it is seen that this would be a requirement that would need to be fulfilled at the time of request. Thus since the user is able to identify a specific printer to print the document at the time of upload it is seen that such an attribute would be checked during the request.

10. Applicant's arguments with respect to the remaining claims are similar to those presented for claim 1 and are addressed similarly.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The factual inquiries set forth in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

14. Claims 1-3, 5, 9-13, 15, 20, 21 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2003/0101342 to Hansen (hereinafter "Hansen") and further in view of US Pat. No. 7248693 to Tretter et al. (hereinafter "Tretter").

15. **As to Claim 1,** Hansen discloses **a file transfer system, comprising:**

a file management server comprising a web page, the file management server being configured to manage access to files stored therein and transfer of the files subject to entry of a first password through the webpage (Paragraph [0025] of Hansen discloses an information holding station located remotely from the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1)**;**

a file transmitting terminal (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1);

a file receiving terminal (Paragraph [0027] of Hansen discloses submitting a request to print a document at a printing station. Figure 1); **and**

a mobile terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1),

wherein

said file management server, said file transmitting terminal, said file receiving terminal, and the mobile terminal are connected to each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link);

said file transmitting terminal is configured to transmit, to said file management server, a particular file and

a second password for accessing the particular file as a part of an authorization condition, through the web page of the file management server (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Paragraph [0033] discloses the secure server includes a website);

said file management server is further configured to store and to correlatingly manage the particular file and the second password transmitted from said file transmitting terminal (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein

the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

said mobile terminal is configured to transfer an address of the file receiving terminal that is permitted to access the particular file stored in the file management server, to said file management server through the web page of the file management server (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said file management server is further configured to store and to correlatingly manage the address of said receiving terminal with the particular file (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said file receiving terminal is further configured to transmit to said file management server a request for transferring the particular file (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310)); **and**

in response to the request transmitted by said file receiving terminal, (i) if an address of the requesting file receiving terminal and the stored address of the file receiving terminal transferred by the mobile terminal are determined match, and (ii) if the request transmitted by said file receiving terminal is determined to include the second password, said file management server transfers the particular file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit

access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)). Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the secure printing system as disclosed by Hansen, with verifying a printer as disclosed by Tretter. One of ordinary skill in the art would have been motivated to combine to use a

known technique to improve similar devices in the same way. The addition of Tretter's disclosure to Hansen would improve the security of the secure printing system.

16. **As to Claim 2,** Hansen-Tretter discloses the invention as claimed as described in claim 1 **wherein**

said authorization condition corresponding to said particular file is said second password for accessing said particular file (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key)**; and**

said file management server is configured to, if a password transmitted with said request by said file receiving terminal matches said password transmitted by said file transmitting terminal, transmit said particular file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))**.**

17. **As to Claim 3,** Hansen-Tretter discloses the invention as claimed as described in claim 1**. wherein**

said authorization condition is one or more user IDs that are authorized to access said particular file (Paragraph [0027] of Hansen discloses the security key comprises a conventional password, digital signature or ID, or some other encryption system in which one or more passwords or signatures are used to create a unique identifier to permit access to the secure document only by the owner/operator of the unique identifier)**; and**

said file management server, is configured to, if a user ID transmitted with said request by said file receiving terminal is included in said one or more user IDs transmitted by said file transmitting terminal, transmit said particular file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Figure 6 discloses the printer securely getting the print job from the server (310))**.**

18. **As to Claim 5,** Hansen-Tretter discloses the invention as claimed as described in claim 1**.**

wherein

said file transmitting terminal is configured to transmit an effective period corresponding to said particular file (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**;**

said file management server is configured to store the corresponding effective period with said particular file (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**; and**

said file management server is configured to, if the corresponding effective period has expired, prohibit said particular file from being transmitted (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**.**

19. **As to Claim 9,** Hansen-Tretter discloses the invention as claimed as described in claim 1 **wherein**

said mobile terminal is configured to acquire the address of said file receiving terminal and to transmit the address to said file management server (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**;**

said file management server is configured to store the address of said file receiving terminal transmitted from said mobile terminal (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**; and**

said file management server is configured to, in response to said request for transmitting said particular file from said file receiving terminal, transmit said particular file to said file receiving terminal if the address of said file receiving terminal matches the stored address (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the

mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

20. **As to Claim 10,** Hansen-Tretter discloses the invention as claimed as described in claim 1, **wherein said file receiving terminal is configured to print or to store, in a recording medium, said particular file received from said file management server** (Figure 6 of Hansen discloses the printer securely getting the print job from the server and printing the document (310)).

21. **As to Claim 11,** Hansen discloses **a file management server connected to a file transmitting terminal, a file receiving terminal, and a mobile terminal via a network, comprising:**

a communication unit configured to exchange data with an external apparatus via said network (Paragraph [0027] of Hansen discloses a mobile computing device communicating with various apparatuses through a network. Figure 1);

a display unit configured to display a web page for transmitting files (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website);

a first storage unit configured to store a particular file and a second password for accessing the particular file as part of an authorization condition, the particular file and the second

password being transmitted by the file transmitting terminal and the second password being associated with the particular file (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1)**;**

a second storage unit configured to store and to correlatingly manage an address of the file receiving terminal that is allowed to access the particular file stored in the first storage unit with the particular file, the address being transmitted from the mobile terminal through the web page of the file management server (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**;**

a file transferring unit configured to, in response to a request for transferring said particular file stored in said first storage unit from said file receiving terminal, transfer said particular file to said file receiving terminal (i) if an address of the requesting file receiving terminal and the stored address of the file receiving terminal transmitted from the mobile terminal are determined to match, and (ii) if the request for transferring said particular file is determined to include the second password is satisfied (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to

identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)) Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

22. **As to Claim 12,** Hansen-Tretter discloses the invention as claimed as described in claim 11**, wherein**

said authorization condition corresponding to said particular file is said second password for accessing said particular file (Paragraph [0027] of Hansen discloses a document being held

at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key)**; and**

said file transferring unit is configured to, if a password transmitted with said request matches said password stored in said first storage unit, transfer said particular file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))**.**

23. **As to Claim 13,** Hansen-Tretter discloses the invention as claimed as described in claim 11 **wherein**

said authorization condition corresponding to said particular file is one or more user IDs (Paragraph [0027] of Hansen discloses the security key comprises a conventional password, digital signature or ID, or some other encryption system in which one or more passwords or signatures are used to create a unique identifier to permit access to the secure document only by the owner/operator of the unique identifier)**; and**

said file transferring unit is configured to, if a user ID transmitted with said request is included in said one or more user IDs stored in said first storage unit, transfer said particular file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting

a security key which is used to only permit access to the secured document only by the owner. Figure 6 discloses the printer securely getting the print job from the server (310)).

24. **As to Claim 15,** Hansen-Tretter discloses the invention as claimed as described in claim 11 **wherein**

said first storage unit is configured to further store an effective period of said particular file (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**; and said file transfer unit is configured to, if the effective period of said particular file has expired, avoid transferring said particular file to said file receiving terminal** (Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station)**.**

25. **As to Claim 20,** Hansen discloses **a file transfer method of an information processing apparatus, comprising the steps of:**

displaying a web page configured to transfer and to receive files (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website)**; storing a particular file and a second password for accessing the particular file as part of an authorization condition, the particular file and the second password being transmitted by said file transfer terminal through the web page, the second password being associated with the particular file** (Paragraphs [0026]-[0027] of Hansen discloses computer workstation

being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1);

storing and correlatingly managing, by the information processing apparatus an address of a file receiving terminal that is allowed to access the particular file with the particular file the address being transmitted from a mobile terminal through the web page (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

receiving a request for transmitting said particular file designated from the file receiving terminal (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310)); **and**

in response to the request, by the information processing apparatus, transmitting said particular file to said file receiving terminal (i) if an address of the requesting file receiving terminal and the stored address of the file receiving terminal transmitted from the mobile terminal are determine to match, and (ii) if the request for transmitting said particular file is determined to include the second password (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))

Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

26. **As to Claim 21,** Hansen discloses **a non-transitory computer-readable storage medium having embedded therein instruction, which when executed by a processor causes the processor to perform the method comprising:**

displaying a web page configured to transfer and to receive files (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website)

storing a particular file and a second password for accessing the particular file as part of an authorization condition, the particular file and the second password being transmitted by said file transfer terminal through the web page and the second password being associated with the particular file (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1);

storing and correlatingly managing an address of a file receiving terminal that is allowed to access the particular file with the particular file the address being transmitted from a mobile terminal through the web page (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

receiving a request for transmitting said particular file designated from the file receiving terminal (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310));

in response to the request, transmitting, said particular file to said file receiving terminal (i) if an address of the requesting file receiving terminal and the stored address of the file receiving terminal transmitted form the mobile terminal are determined to match, and (ii) if the request for transmitting said particular file is determine to include the second password (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the

mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)) Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

27. **As to Claim 30,** Hansen discloses **an image forming apparatus connected with a stored document management server and a user terminal via a network, comprising:**

a communication unit configured to exchange data via said network and, subject to entry of a first password, to transmit a stored particular document and a second password for accessing the particular document to the stored document management server, the second password being associated with the particular document (Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1. Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly)**;**

a storage unit configured to store a particular document and the second password associated with the particular document as a part of an authorization condition for accessing said stored particular document (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly)**; and**

an image forming unit configured to print said stored particular document (Figure 6 of Hansen discloses the printer securely getting the print job from the server and printing it (310))**;**

wherein

said communication unit is configured to, in response to reception of a request for transmitting said particular stored document from said user terminal transmit said stored particular document and second password to said stored document management server, (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)), **the stored document management server being configured to store and correlatingly manage an address of a particular file receiving terminal that is permitted to access the stored particular document with the stored particular document** (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer).

Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server.

Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

28. Claims 22-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hansen and further in view of Tretter and further in view of US Pat. No. 7130069 to Honma (hereinafter "Honma")

29. **As to Claim 22,** Hansen discloses **an image forming system, comprising: a stored document management server comprising a web page, the stored document management server being configured to manage access to documents stored therein and transfer of the stored documents subject to entry of a first password through the web page** (Paragraph [0025] of Hansen discloses an information holding station located remotely from the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1);

a first [image forming] apparatus (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1);

a second image forming apparatus (Paragraph [0027] of Hansen discloses submitting a request to print a document at a printing station. Figure 1)**; and**

a mobile terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1),

wherein

said stored document management server, said first image forming apparatus, and said second image forming apparatus, and said mobile terminal are connected to each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link)**;**

said first image forming apparatus is configured to transmit, to said stored document management server,

a particular document (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Paragraph [0033] discloses the secure server includes a website) **and**

a second password for accessing the particular document as a part of an authorization condition, through the web page of the stored document management server (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document

electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Paragraph [0033] discloses the secure server includes a website);

said stored document management server is further configured to store and to correlatingly manage the transmitted particular document and the second password transmitted form the first image forming apparatus (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly);

said mobile terminal is configured to transfer an address of the second image forming apparatus that is permitted to access the particular document stored in the stored document management server, to said stored document management server through the web page of the stored document management server (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said stored document management server is further configured to store and to correlatingly manage the address of said second image forming apparatus with the stored particular document (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer);

said second image forming apparatus is further configured to transmit to said stored document management server a request for transferring the stored particular document (Figure 6 of Hansen discloses the printer securely getting the print job from the server (310)); **and**

in response to the request transmitted by the second image forming apparatus, (i) if an address of the requesting second image forming apparatus and the stored address of the second image forming apparatus transferred by the mobile terminal are determined to match, and (ii) if the request for transferring the stored particular document is determine to include the second password is satisfied, said stored document management server, is configured to transfer the stored particular document to said second image forming apparatus (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

Hansen does not explicitly disclose the first apparatus being **image forming.**

However, Honma discloses this. Column 17 lines 13-30 of Honma disclose a user being able to use an original image forming apparatus to access another image forming apparatus to obtain a document to print out on the original image forming apparatus.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the printing system as disclosed by Hansen, with having one image forming apparatus transfer to another as disclosed by Honma. One of ordinary skill in the art would have been motivated to combine to apply simple substitution of one known element for another to obtain predictable results. Honma discloses it is well known in the art to have one image forming apparatus provide a document to another image forming apparatus. Hansen discloses obtaining the document information from a computer work station. Thus it would have been simple substitution of one known element for another to implement such a feature in Hansen.

Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

30. **As to Claim 23,** Hansen discloses **a stored document management server connected to a first image forming apparatus, a second image forming apparatus, and a mobile terminal via a network, comprising:**

a communication unit configured to exchange data with said first and second image forming apparatuses via said network (Paragraph [0027] of Hansen discloses a mobile computing device communicating with various apparatuses through a network. Figure 1)**;**

a display unit configured to display a web page for transmitting stored documents (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station. Paragraph [0033] discloses the secure server utilizes a website)**;**

a first storage unit configured to store a particular document and a second password for accessing the particular document as part of an authorization condition the stored particular document and the second password being transmitted by the first [image forming] apparatus and the second password being associated with the stored particular document (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1)**;**

a second storage unit configured to store and correlatingly manage an address of the second image forming apparatus that is allowed to access the stored particular document with the stored particular document, the address being transmitted from the mobile terminal through the web page of the stored document management server (Paragraph

[0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer); **and**

a stored document transferring unit configured to, in response to a request for transferring said particular document stored in said first storage unit from said second image forming apparatus, transfer said stored particular document to said second image forming apparatus (i) if an address of the requesting second image forming apparatus and the stored address of the second image forming apparatus transmitted form the mobile terminal is determined to match, and (ii) if the request for transferring said stored particular document includes the second password (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))

Hansen does not explicitly disclose the first apparatus being **image forming.**

However, Honma discloses this. Column 17 lines 13-30 of Honma disclose a user being able to use an original image forming apparatus to access another image forming apparatus to obtain a document to print out on the original image forming apparatus.

Examiner recites the same rationale to combine used in claim 22.

Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

31. **As to Claim 24,** Hansen discloses **an image forming system, comprising: a first image forming apparatus configured to manage access to documents stored therein and transfer of the stored documents subject to entry of a first password** (Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login

function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1)**, to store a particular document and a second password for accessing the stored particular document,** (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly) **and to store and to correlatingly manage an address of a second image forming apparatus that is permitted to access the stored particular document with the stored particular document** (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer) **the stored particular document and the second password being transmitted by another [image forming] apparatus and the second password being associated with the stored particular document** (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Figure 1)**;**

a user terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1)**; and**

the second image forming apparatus (Paragraph [0025] of Hansen discloses the secure server acts to hold documents in storage and communicates with one or more printing stations)**;**

wherein

said first image forming apparatus, said user terminal, and said second image forming apparatus are connected to each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link)**;**

in response to a request from said user terminal, said first image forming apparatus is configured to, if the request from said user terminal is determined to include the second password, transmit said stored particular document and said second password for accessing the particular document as a part of an authorization condition to said second image forming apparatus (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310))**; and**

said second image forming apparatus is configured to store said particular document and said second password associated with the stored particular document and, if a received request for printing said stored document is determined to include said second password, to print said stored particular document (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer.

Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

Hansen does not explicitly disclose the another apparatus being **image forming.**

However, Honma discloses this. Column 17 lines 13-30 of Honma disclose a user being able to use an original image forming apparatus to access another image forming apparatus to obtain a document to print out on the original image forming apparatus.

Examiner recites the same rationale to combine used in claim 22.

Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

32. **As to Claim 25,** Hansen discloses **an image forming system, comprising:**

a first image forming apparatus configured to manage access to document stored therein and transfer of the stored documents subject to entry of a first password (Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1)**, and to store a particular document and a second password for accessing the particular document, the second password being associated with the stored particular document** (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly)**;**

a stored document management server (Paragraph [0025] of Hansen discloses an information holding station located remotely from the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1)**;**

a user terminal (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1); **and**

a second image forming apparatus (Paragraph [0025] of Hansen discloses the secure server acts to hold documents in storage and communicates with one or more printing stations); **wherein**

said first image forming apparatus, said stored document management server, said user terminal, and said second image forming apparatus are connected each other via a network (Figure 1 of Hansen discloses all the components being in connected via a network communication link);

in response to a request from said user terminal, said first [image forming] apparatus is configured to, if the request from said user terminal is determined to include said second password, transmit said particular stored document and said second password as part of an authorization condition to said stored document management server (Paragraphs [0026]-[0027] of Hansen discloses computer workstation being used to send a document electronically to information holding station. Paragraph [0028] discloses pre-identifying the security key to be used for printing the document. Paragraph [0033] discloses the secure server includes a website);

said stored document management server is configured to store said particular document and said second password, and to store and to correlatingly manage an address of a second image forming apparatus that is permitted to access the stored particular document with the stored particular document (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph

[0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly); **and,**

in response to a request for transmitting said stored particular document from said second image forming apparatus, (i) if an address of the requesting second image forming apparatus and the stored address of the second image forming apparatus that is permitted to access the stored particular document are determined to match, and (ii) if the request transmitted by the second image forming apparatus is determined to include the second password, said stored document management server is configured to transmit said particular stored document to said second image forming apparatus (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)); **and said second image forming apparatus is configured to print said stored document transmitted from said stored document management server** (Figure 6 of Hansen discloses the printer securely getting the print job from the server and printing it (310)).

Hansen does not explicitly disclose the first apparatus being **image forming.**

However, Honma discloses this. Column 17 lines 13-30 of Honma disclose a user being able to use an original image forming apparatus to access another image forming apparatus to obtain a document to print out on the original image forming apparatus.

Examiner recites the same rationale to combine used in claim 22.

Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

33. **As to Claim 26,** Hansen discloses **an image forming apparatus connected with another image forming apparatus via a network, comprising:**
a communication unit configured to exchange data via said network, and, subject to entry of a first password, to receive a particular document and a second password for accessing the particular document from said other image forming apparatus, the second password being transmitted by the other image forming apparatus and being associated with the

particular document (Paragraph [0025] of Hansen discloses an information holding station located with the printing station. This station includes a secure server to hold documents in storage and supply documents for printing upon requests. Information holding station acts as a network printing manager to handle printing requests among one or more printing stations. Paragraph [0031] discloses password/login function permits confidential access to the printing system and paragraph [0033] discloses the secure server includes a website. Figure 1. Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly) **and the other image forming apparatus being configured to store and correlatingly manage an address of a particular image forming apparatus that is permitted to access the particular document with the stored particular document** (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**;**

a storage configured to store the particular document and the second password associated with the particular document as part of an authorization condition for accessing said stored particular received from said other image forming apparatus (Paragraph [0027] of Hansen discloses a document being held at the server for printing. Wherein the document is accessed via a security key and paragraph [0028] discloses pre-identifying the security key. Thus the server holds the document and the key correlatingly)**;**

an operations input unit (Paragraph [0030] of Hansen discloses a user interface displaying a printing menu to enable communication with information holding station)**; and**

an image forming unit configured to, in response to reception of a request for printing said stored particular document, if the request for printing said stored particular document includes the second password, print said stored particular document (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server and printing it (310))**.** Hansen does not explicitly disclose the first apparatus being **image forming.**

However, Honma discloses this. Column 17 lines 13-30 of Honma disclose a user being able to use an original image forming apparatus to access another image forming apparatus to obtain a document to print out on the original image forming apparatus.

Examiner recites the same rationale to combine used in claim 22.

Hansen in view of Tretter more clearly discloses the feature of verifying a printer to be the correct printer for a request.

Column 4 lines 49-54 of Tretter discloses before the order can be carried out, the customer is asked to identify the secure printer to which the documents will be delivered. This will allow the server to communicate with the secure printer. If the secure printer has a URL, the customer may enter the URL of the secure printer. Column 5 lines 14-20 disclose the secure

printer then established its identity with the server by sending the public key KA to the server. Column 5 lines 45-59 disclose after the identity of the secure printer has been authenticated, the server accesses the file X of the ordered document and sends it to the printer. This process is done with respect to a smart card providing identification to the printer. However, column 8 lines 23-25 disclose the cryptographic keys may be embedded in the ROM of the printer. Thus, the printer becomes trusted, not the holder of the smart card. According to this embodiment it is clearly seen that the printer is verified to be the correct printer.

Examiner recites the same rationale to combine used in claim 1.

34. **As to Claim 27,** Hansen-Tretter discloses the invention as claimed as described in claim 26**, wherein**

said image forming apparatus is further connected to a user terminal via said network (Paragraph [0027] of Hansen discloses a mobile computing device. Figure 1)**; and**

said communication unit is configured to, in response to a transfer request from said user terminal, if said transfer request satisfies said authorization condition, transmit said stored particular document and said authorization condition stored in said storage unit to a destination (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this

criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

35. **As to Claim 28,** Hansen-Tretter discloses the invention as claimed as described in claim 27**, wherein said transfer request includes said destination, the second password as said authorization information for accessing said stored particular document, and a registration code of said stored particular document that said communication unit has received from said user terminal via said network** (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

36. **As to Claim 29,** Hansen-Tretter discloses the invention as claimed as described in claim 27**, wherein said transfer request includes said destination, said authorization condition for accessing said stored particular document, and a registration code of said stored particular document** that **are input by said operations input unit** (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph

[0031] discloses an identify printer function that permits the user to identify a specific printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

37. Claims 6-8 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hansen-Tretter and further in view of US Pat. No. 6785812 to Botham, Jr. et al. (hereinafter "Botham").

38. **As to Claim 6,** Hansen-Tretter discloses the invention as claimed as described in claim 5. Hansen-Tretter does not explicitly disclose**, wherein said file management server is configured to, if the corresponding effective period has expired, delete said particular file**

However, Botham discloses this. Column 4 lines 34-36 of Botham discloses destroying a document once its allotted lifetime has expired**.**

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the invention of claim 5 as disclosed by Hansen-Tretter, with deleting a file after a period as disclosed by Botham. One of ordinary skill in the art would have been motivated to combine to apply a known technique to a know device ready for improvement to yield predictable results. Paragraph [0029] of Hansen discloses time (duration, time of day, day of week, etc) can be used as a factor in determining whether to allow selective printing at printing station. Accordingly it would have been obvious to implement deleting the file after the time has expired, since it is seen to be a known technique used in view of utilizing time as a factor in printing.

39. **As to Claim 7,** Hansen-Tretter discloses the invention as claimed as described in claim 1. Hansen-Tretter does not explicitly disclose **wherein**

said file transmitting terminal is configured to transmit an effective number of transfers corresponding to said particular file;

said file management server is configured to store the corresponding effective number of transfers with said particular file; and

said file management server is configured to, if the number of transfers of said particular file reaches the corresponding effective number of transfers, prohibit said particular file from being transmitted.

However, Botham discloses this (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Then based on purpose of setting a maximum number of times a document may be printed it is inherent that when a file reaches the effective number, it will no longer be distributed)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the system of claim 1 as disclosed by Hansen-Tretter, with having a maximum number of times a document may be printed as disclosed by Botham. One of ordinary skill in the art would have been motivated to combine to make document distribution more secure and controllable (column 2 lines 18-65 of Botham).

40. **As to Claim 8,** Hansen-Tretter-Botham discloses the invention as claimed as described in claim 7**, wherein said file management server is configured to, if the number of transfers of said particular file reaches the corresponding effective number of transfers, delete said particular file** (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Thus it is seen that when a document has been viewed/printed the maximum number of times it is essentially no longer accessible, thus it would be obvious to delete the document in order to preserve space on the file management server)**.**

Examiner recites the same rationale to combine used in claim 7.

41. **As to Claim 16,** Hansen-Tretter discloses the invention as claimed as described in claim 15. Hansen-Tretter does not explicitly disclose**, wherein said file transferring unit is configured to, if the effective period of said particular file has expired, delete said particular file**

However, Botham discloses this. Column 4 lines 34-36 of Botham discloses destroying a document once its allotted lifetime has expired**.**

Examiner recites the same rationale to combine used in claim 6.

42. **As to Claim 17,** Hansen-Tretter discloses the invention as claimed as described in claim 11**.** Hansen-Tretter does not explicitly disclose **wherein**
said first storage unit is configured to further store an effective number of transfers of said particular file; and

said file transfer unit is configured to, if the number of transfers of said particular file reaches the effective number stored in said first storage unit, avoid transferring said particular file to said file receiving terminal.

However, Botham discloses this (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Then based on purpose of setting a maximum number of times a document may be printed it is inherent that when a file reaches the effective number, it will no longer be distributed)

Examiner recites the same rationale to combine used in claim 7.

43. **As to Claim 18,** Hansen-Tretter-Botham discloses the invention as claimed as described in claim 17**, wherein said file transferring unit is configured to, if the number of transfers of said particular file reaches the effective number, delete said particular file** (Column 2 lines 45-55 of Botham disclose being able define control characteristics, including allowing a document to only be viewed or printed a maximum number of times. Thus it is seen that when a document has been viewed/printed the maximum number of times it is essentially no longer accessible, thus it would be obvious to delete the document in order to preserve space on the file management server)**.**

Examiner recites the same rationale to combine used in claim 7.

44. Claims 4, 14 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hansen-Tretter and further in view of US Pat. No. 6233618 to Shannon (hereinafter "Shannon").

45. **As to Claim 4,** Hansen-Tretter n discloses the invention as claimed as described in claim 1. Hansen-Tretter does not explicitly disclose **wherein**

said authorization condition is the membership of a group that is authorized to access said particular file; and

said file management server is configured to, if a user ID transmitted with said request by said file receiving terminal is a member of said group, transmit said particular file to said file receiving terminal.

However, Shannon discloses this. Column 7 lines 58-68 of Shannon disclose a user of a particular group being restricted from viewing particular pages.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the system of claim 1 as disclosed by Hansen-Tretter, with using membership of a group as the authorization condition as disclosed by Shannon. One of ordinary skill in the art would have been motivated to combine to improve access and control capabilities (column 3 lines 35-45 of Shannon).

46. **As to Claim 14,** Hansen-Tretter discloses the invention as claimed as described in claim 11. Hansen-Tretter does not explicitly disclose **further comprising a third storage unit configured to store a group name and user IDs of group members;**

wherein

said authorization condition stored in said first storage unit is said group name; and

said file transferring unit is configured to, if a user ID transmitted with said request is included in said group members, transfer said particular file to said file receiving terminal.

However, Shannon discloses this. Column 7 Table 1 discloses a storage associating Clients with their groups. Column 7 lines 58-68 of Shannon disclose a user of a particular group being restricted from viewing particular pages

Examiner recites the same rationale to combine used in claim 4.

47. **As to Claim 19,** Hansen-Tretter-Shannon discloses the invention as claimed as described in claim 14 **wherein**

said second storage unit is configured to store the address of said file receiving terminal transmitted from the mobile terminal (Paragraph [0027] of Hansen disclose the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific printer)**, and**

said file transferring unit is configured to, in response to the request for transferring said particular file, said request transmitted from said file receiving terminal, only if the address of said file receiving terminal matches an address stored in said second storage unit, transmit said particular file to said file receiving terminal (Paragraph [0027] of Hansen discloses submitting a security key which is used to only permit access to the secured document only by the owner. Paragraph [0027] further discloses the mobile device transmits printing instructions which specify how, when and where the document will be printed. Furthermore paragraph [0031] discloses an identify printer function that permits the user to identify a specific

printer. Accordingly it is seen that this criteria would also need to be met. Figure 6 discloses the printer securely getting the print job from the server (310)).

Conclusion

48. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

49. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 5835922 A - Document processing apparatus and method for inputting the requirements of a reader or writer and for processing documents according to the requirements to Shima; Yoshihiro et al.

US 6914687 B1 - Data processing apparatus and image recording apparatus, method for controlling data processing apparatus and method for controlling image recording apparatus, and storage medium to Hosoda; Yuichi et al.

US 20030076526 A1 - Method and apparatus for printing documents using a document repository in a distributed data processing system to Gopalan, Prabhakar

US 6931432 B1 - Data transmission apparatus and method with control feature for transmitting data or transmitting a storage location of data to Yoshida; Hiroyoshi

US 7190475 B2 - Method for providing a print and apparatus to Nomoto; Tetsushi

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN S. MAI whose telephone number is (571)270-5001. The examiner can normally be reached on Monday - Friday, 8am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/K. S. M./
Examiner, Art Unit 2456

/KEVIN BATES/
Primary Examiner, Art Unit 2456